

UNITED STATES DISTRICT COURT

for the
Western District of Washington

In the Matter of the Search of

*(Briefly describe the property to be searched
or identify the person by name and address)*Business operating as Technology Express; a Maroon
2014 Land Rover Evoque; one Samsung phone and one
iPhone;

Case No.

MJ17-244

FILED
LODGED
JUN 12 2017
AT SEATTLE
CLERK U.S. DISTRICT COURT
BY WESTERN DISTRICT OF WASHINGTON
DEPUTY
ENTERED
RECEIVED

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:

See Attachments A-1 to A-4, which are incorporated herein by reference

located in the Western District of Washington, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachments B-1 to B-4, which are incorporated herein by reference

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section

Offense Description

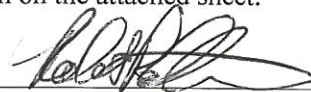
18 U.S.C. Sec. 1956, 1960

Money Laundering; Unlicensed Money Transmitting

The application is based on these facts:

Affidavit of HSI Special Agent Robert Patterson

- ☒ Continued on the attached sheet.
- ☐ Delayed notice of days (give exact ending date if more than 30 days:) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.



Applicant's signature

HSI Special Agent Robert Patterson

Printed name and title

Sworn to before me and signed in my presence.

Date:

June 12, 2017



Judge's signature

City and state: Seattle, WA

Magistrate Judge Mary Alice Theiler

Printed name and title

1 support the issuance of the requested warrants. When the statements of others are set
2 forth in this affidavit, they are set forth in substance and in part.

3 **PURPOSE OF AFFIDAVIT**

4 3. This affidavit is submitted in support of an application for search warrants
5 for the following:

6 a. The premises of the business known as "Technology Express,"
7 located at 16130 Woodinville-Redmond Road, Unit 1, Woodinville, Washington (the
8 "**Subject Business**"), as more fully set forth in Attachment A-1, which is incorporated
9 herein by reference. I seek authority to search for the items set forth in Attachment B-1,
10 which is incorporated herein by reference.

11 b. A maroon 2013 Land Rover Evoque, personalized Washington
12 license plate MICHAIL, registered to Michail Wilson ("Wilson"), 12721 50th Ave SE,
13 Everett, Washington 98208, Vehicle Identification Number SALVT1BG8DH810540 (the
14 "**Target Vehicle**"), as more fully set forth in Attachment A-2, which is incorporated
15 herein by reference. I seek authority to search for the items set forth in Attachment B-2,
16 which is incorporated herein by reference.

17 c. A Samsung phone belonging to Michail Wilson (the "**Samsung**
18 **Phone**"), as more fully set forth in Attachment A-3, which is incorporated herein by
19 reference. I seek authority to search for the items set forth in Attachment B-3, which is
20 incorporated herein by reference.

21 d. An Apple iPhone phone belonging to Michail Wilson (the "**Apple**
22 **iPhone**"), as more fully set forth in Attachment A-4, which is incorporated herein by
23 reference. I seek authority to search for the items set forth in Attachment B-4, which is
24 incorporated herein by reference.

25 4. This affidavit is also submitted in support of an application for a combined
26 criminal and civil forfeiture seizure warrant for the following assets:

27 //

1 a. The **Target Vehicle**.

2 b. All bitcoins stored in or accessible via the Mycelium bitcoin wallets
3 belonging to Michail Wilson (the "Mycelium Wallets") that are accessible via the
4 **Samsung Phone** or the **Apple iPhone** (the "**Mycelium Bitcoins**"), as described in
5 Attachments C and D, which are incorporated herein by reference.

6 5. For the reasons set forth herein, I submit that there is probable cause to
7 believe that searches of the **Subject Business**, the **Target Vehicle**, the **Samsung Phone**,
8 and the **Apple iPhone** will reveal evidence, contraband, fruits, and instrumentalities of
9 violations of 18 U.S.C. § 1956 (money laundering) and 18 U.S.C. § 1960 (conducting an
10 unlicensed money transmitting business).

11 6. I additionally submit that there is probable cause to believe that the **Target**
12 **Vehicle** and the **Mycelium Bitcoins** constitute property involved in a transaction or
13 attempted transaction in violation of 18 U.S.C. § 1956 and 18 U.S.C. § 1960, or are
14 traceable to such property. The **Target Vehicle** and the **Mycelium Bitcoins** are,
15 therefore, subject to forfeiture to the United States pursuant to 18 U.S.C. § 981(a)(1)
16 (civil forfeiture).

17 7. I further submit that there is probable cause to believe that the **Target**
18 **Vehicle** and the **Mycelium Bitcoins** constitute property involved in a violation of 18
19 U.S.C. § 1956 and 18 U.S.C. § 1960, or are traceable to such property. The **Target**
20 **Vehicle** and the **Mycelium Bitcoins** are, therefore, subject to forfeiture to the United
21 States pursuant to 18 U.S.C. § 982(a)(1) (criminal forfeiture).

22 8. I moreover submit that there is probable cause to believe that the **Mycelium**
23 **Bitcoins** constitute (1) money, negotiable instruments, securities or other things of value
24 furnished or intended to be furnished in exchange for a controlled substance in violation
25 of the Controlled Substances Act; (2) proceeds traceable to such an exchange; or (3)
26 money, negotiable instruments, or securities used and intended to be used to facilitate a
27 violation of the Controlled Substances Act. The **Mycelium Bitcoins** are therefore subject
28 to forfeiture to the United States pursuant to 21 U.S.C. § 881(a)(6) (civil forfeiture).

Affidavit of Special Agent Patterson - 3
USAO 201501195

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

1 9. Finally, I submit that there is probable cause to believe that the **Target**
 2 **Vehicle** and the **Mycelium Bitcoins** constitute property constituting, or derived from,
 3 any proceeds obtained, directly or indirectly, as the result of drug trafficking, and are
 4 therefore subject to forfeiture to the United States pursuant to 21 U.S.C. § 853(a)
 5 (criminal forfeiture).

6 10. As property subject to forfeiture, the **Target Vehicle** and the **Mycelium**
 7 **Bitcoins** may be seized pursuant to 18 U.S.C. § 981(b) and 21 U.S.C. § 853(f).

8 11. With respect to seizure, 21 U.S.C. § 853(f) specifically provides that a court
 9 may issue a criminal seizure warrant when it “determines that there is probable cause to
 10 believe that the property to be seized would, in the event of conviction, be subject to
 11 forfeiture and that a[] [protective] order under [21 U.S.C. § 853(e)] may not be sufficient
 12 to assure the availability of the property for forfeiture.” For the reasons described below,
 13 I submit that a protective order under 21 U.S.C. § 853(e) would not be sufficient to assure
 14 the availability of the **Target Vehicle** or the **Mycelium Bitcoins** for forfeiture.

15 12. As further set forth below, there is a substantial risk that the **Mycelium**
 16 **Bitcoins** will dissipate or otherwise become unavailable for forfeiture unless immediate
 17 steps are taken, upon the execution of the requested searches, to secure the **Mycelium**
 18 **Bitcoins**. Thus, I seek authority to (1) compel Michail Wilson to put one or more of his
 19 fingers on the **Samsung Phone** and **Apple iPhone** to unlock the devices; and (2) access
 20 the Mycelium Wallets via the Mycelium applications on the **Samsung Phone** and the
 21 **Apple iPhone** for the purpose of transferring all of the **Mycelium Bitcoins** stored in or
 22 accessible via the Mycelium Wallets to a law enforcement-controlled bitcoin wallet.¹
 23 The seized **Mycelium Bitcoins** will then be preserved pending further forfeiture
 24 proceedings.

25
 26
 27 ¹ Per this affidavit and the associated warrant applications, the government also seeks authorization to search both
 28 the **Samsung Phone** and the **Apple iPhone**, for, *inter alia*, any additional bitcoin wallet applications—whether
 associated with Mycelium or not—for the purpose of seeking an immediate follow-up warrant(s), if appropriate, as
 to bitcoins stored in, or otherwise accessible via, said wallet applications.

OVERVIEW OF WILSON'S CONDUCT

13. As set forth below, Michail Wilson is engaged in the business of accepting cash from customers in exchange for transmitting bitcoins to particular digital wallets that are specified by his customers. As the result of the nature of Wilson's business, he is required to register with, and obtain a license from, federal and state authorities. Wilson is aware of these requirements and yet has refused to comply. In addition, Wilson has repeatedly demonstrated a willingness to conduct transactions involving funds that are tainted by criminal activity—for example, by acquiring cash or bitcoins that Wilson knows, or believes to be, the proceeds of criminal activities. As the result of Wilson's conduct, he has engaged in money laundering, in violation of 18 U.S.C. § 1956, and conducting an unlicensed money transmission business, in violation of 18 U.S.C. § 1960.

BACKGROUND ON BITCOIN AND MYCELIUM

14. Digital currency (also known as crypto-currency) is generally defined as an electronically sourced unit of value that can be used as a substitute for fiat currency (*i.e.*, currency created and regulated by a government). Digital currency is not issued by any government, bank, or company; it is instead generated and controlled through computer software operating on a decentralized peer-to-peer network. Digital currency is not illegal in the United States.

15. Bitcoin is a type of digital currency. Bitcoin payments are recorded in a public ledger that is maintained by peer-to-peer verification and is thus not maintained by a single administrator or entity. Bitcoins are widely used to conduct both legitimate and unlawful business. For example, Microsoft accepts bitcoins as payment for Xbox games and services. On the other hand, bitcoins were the payment used on the Silk Road, a website on the dark web that offered drugs and other contraband for sale.

16. Individuals can acquire bitcoins through bitcoin exchanges (*i.e.*, websites that allow individuals to purchase bitcoins for other currency), bitcoin ATMs, or directly from other people. Individuals can also acquire bitcoins by "mining" bitcoins. An individual can mine bitcoins by allowing his/her computing power to verify and record

1 the bitcoin payments into a public ledger. Individuals are rewarded for this task by being
2 given newly created bitcoins.

3 17. An individual can send and receive bitcoins through peer-to-peer digital
4 transactions or by using a third-party broker. Such transactions can be done on many
5 types of computers, including laptop computers and smart phones.

6 18. Even though the public addresses of those engaging in bitcoin transactions
7 are recorded on the public ledger, the true identities of the individuals or entities behind
8 the public addresses are not recorded. If, however, a real individual or entity is linked to
9 a public address, it would be possible to determine what transactions were conducted by
10 that individual or entity. Bitcoin transactions are, therefore, described as
11 "pseudonymous," meaning they are partially anonymous.

12 19. Bitcoins can be stored in digital "wallets." A digital wallet essentially
13 stores the access code that allows an individual to conduct bitcoin transactions on the
14 public ledger. To access bitcoins on the public ledger, an individual must use a public
15 address (or "public key") and a private address (or "private key"). The public address
16 can be analogized to an account number while the private key is like the password to
17 access that account.

18 20. Bitcoin exchangers and bitcoin users often store bitcoins in several ways,
19 including desktop, mobile, and online wallets; hardware devices; and paper wallets. The
20 desktop, mobile, and online application wallets are electronic in nature and can be stored
21 on mobile devices (phones or tablets) or accessed through website-based wallets via a
22 computer, tablet, or any device that can search the internet. Bitcoin wallets can also be
23 stored on external hardware wallets or removable media (such as USB thumb drives,
24 Trezor, Ledger, *etc.*). Each electronic bitcoin application wallet (such as Mycelium) can
25 hold several unique alphanumeric character bitcoin wallet addresses that in turn can hold
26 bitcoin. In addition, paper bitcoin wallets contain a bitcoin address and a QR code with
27
28

1 the public and private key embedded in the code.² Paper wallet keys are not stored
2 digitally. Bitcoin wallets can also be backed up onto paper printouts, USB drives, CDs
3 and accessed through a “seed phrase” (random words strung together in a phrase) or a
4 complex password. Additional security safeguards for bitcoin wallets can include two-
5 feature authorization (such as a password and a phrase).

6 21. Mycelium is a company that offers a bitcoin wallet service. Users of
7 Mycelium’s service generally download a Mycelium application to their smart phone. A
8 user typically accesses the application through a user-generated PIN code. Users can
9 store, receive, and transfer bitcoins via the Mycelium application. Mycelium’s website
10 indicates that Mycelium does not store the private keys that are necessary to access
11 bitcoins on remote servers. Rather, the keys are stored on the device on which the
12 application is installed or any backup created by the user.

13 22. On or about April 12, 2017, a United States Postal Inspector sent an inquiry
14 to Mycelium about whether the company would accept a court order or subpoena.
15 Mycelium responded:

16 I'm not sure if we would be able to help you in any way, as we just create
17 an app for users to download and use on their own phones. We have no
18 way of tracking what they do with the app from our end. Any information
19 we do have is already public on the blockchain and you can look it up on
services like blockchain.info. Sorry we can't be of much help.

20 23. In light of Mycelium’s response, it does not appear that Mycelium could
21 assist in seizing or “freezing” bitcoins associated with a particular user. Rather, law
22 enforcement would need to seize the wallet from the user directly, namely by seizing the
23 user’s cell phone or other digital device housing the wallet, accessing the wallet, and
24 transferring the bitcoins to a law enforcement-controlled bitcoin wallet.

25 //

26 //

27 _____

28 ² A “QR code” is a matrix barcode that is a machine-readable optical label.

SUMMARY OF LAW

A. Unlicensed Money Transmitting Business

24. Title 18, United States Code, Section 1960(a), makes it a crime to knowingly conduct, control, manage, supervise, direct, or own all or part of an unlicensed money transmitting business. The term “money transmitting,” as defined the statute, “includes transferring funds on behalf of the public by any and all means including but not limited to transfers within this country or to locations abroad by wire, check, draft, facsimile, or courier.” *Id.* § 1960(b)(2).

25. Section 1960 sets forth three prongs under which a business constitutes an “unlicensed money transmitting businesses.” First, § 1960(b)(1)(A) makes it a crime to operate a money transmitting business without an appropriate state license where one is required. Second, § 1960(b)(1)(B) makes it a crime to operate a money transmitting business without registering with federal authorities if required by federal regulation. Finally, § 1960(b)(1)(C) makes it a crime to operate a money transmitting business—whether licensed by any authority or not—that “involves the transportation or transmission of funds that are known to the defendant to have been derived from a criminal offense or are intended to be used to promote or support unlawful activity.”

26. The term “specified unlawful activity” includes a wide variety of federal offenses, including drug trafficking. *See* 18 U.S.C. § 1956(c)(7).

27. As set forth below, I submit that Michail Wilson has violated all three prongs of § 1960.

a. The First Prong

28. As set forth above, § 1960(b)(1)(A) makes it a crime to operate a money transmitting business without an appropriate state license where one is required. The State of Washington requires such a license when a person engages in the business of accepting cash in exchange for transmitting bitcoins to a designated bitcoin wallet. Specifically, § 19.230.30(1)(a) of the Washington State Code provides that “[a] person may not engage in the business of money transmission, or advertise, solicit, or hold itself

1 out as providing money transmission, unless the person is . . . [l]icensed as a money
 2 transmitter.” “Money transmission” in turn means “receiving money or its equivalent
 3 value to transmit, deliver, or instruct to be delivered the money or its equivalent value to
 4 another location, inside or outside the United States, by any means including but not
 5 limited to by wire, facsimile, or electronic transfer.” *Id.* § 19.230.10(18).

6 29. The Washington Department of Financial Institutions (“DFI”) has issued
 7 interim regulatory guidance that “[p]ersons engaged in the business of buying or selling
 8 virtual currency fall under the definition of money transmission in the Act.” *See Interim*
 9 *Regulatory Guidance on Virtual Currency Activities 2* (December 8, 2014). The DFI
 10 specifically addressed the following situation:

11 [T]he buyer of virtual currency provides sovereign currency to a business
 12 that either holds value in the form of a desired virtual currency or who upon
 13 receipt of sovereign currency executes a purchase of the virtual currency
 14 from another source. In either case the business ultimately transmits virtual
 15 currency value to the buyer. The value is transmitted to a wallet location
 16 either designated by the buyer or generated by the business.

17 *Id.* at 3. The DFI clarified that this type of transaction constitutes “money transmission
 18 and the business must hold a Washington money transmitter license when providing the
 19 service to Washington residents.” *Id.*

20 30. On or about March 25, 2015, and again on or about October 25, 2016, DFI
 21 told HSI Seattle that neither Wilson nor his company, Technology Express, is licensed to
 22 conduct the activity described herein. Moreover, as set forth below, Wilson repeatedly
 23 has indicated that he has not registered his business.

24 **b. The Second Prong**

25 31. The second prong of § 1960 makes it a crime to operate a money
 26 transmitting business without registering with federal authorities if required by federal
 27 regulation. 18 U.S.C. § 1960(b)(1)(B).

28 32. The U.S. Department of the Treasury’s Financial Crimes Enforcement
 Network (“FinCEN”) has stated that an exchanger of a virtual currency like bitcoin is

1 required to register as a money service business (“MSB”) with FinCEN. *See Application*
 2 *of FinCEN’s Regulations to Persons Administering, Exchanging, or Using Virtual*
 3 *Currencies*, FIN-2013-G001, Department of the Treasury, Financial Crimes Enforcement
 4 Network (March 18, 2013) (hereinafter “FinCEN Guidance”). Specifically, FinCEN’s
 5 regulations provide that a MSB includes businesses operating as a “money transmitter.”
 6 31 C.F.R. § 1010.100(ff)(5). A “money transmitter,” in turn, means “the acceptance of . .
 7 . funds . . . from one person and the transmission of . . . funds . . . to another location or
 8 person by any means.” *Id.* § 1010.100ff(5)(i)(A). FinCEN has clarified that the
 9 “definition of a money transmitter does not differentiate between real currencies and
 10 convertible virtual currencies,” such as bitcoin. *See* FinCEN Guidance at 3.

11 33. On or about March 23, 2017, an agent queried FinCEN and learned that
 12 neither Wilson nor his company have registered as MSBs with FinCEN.

13 c. **The Third Prong**

14 34. Finally, the third prong of § 1960 provides that it is unlawful to operate a
 15 money transmitting business that “otherwise involves the transportation or transmission
 16 of funds that are known to the defendant to have been derived from a criminal offense or
 17 are intended to be used to promote or support unlawful activity.” 18 U.S.C.
 18 § 1960(b)(1)(C).

19 35. As set forth below, Wilson has demonstrated a repeated willingness to deal
 20 in funds that Wilson knows to have been derived from or are intended to promote or
 21 support unlawful activity, including drug trafficking.

22 **B. Money Laundering**

23 36. Title 18, United States Code, Section 1956 provides that it is a crime for:

24 (1) Whoever, knowing that the property involved in a financial transaction
 25 represents the proceeds of some form of unlawful activity, conducts or
 26 attempts to conduct such a financial transaction which in fact involves the
 proceeds of specified unlawful activity—

27 //

1 (A)

2 (i) with the intent to promote the carrying on of specified unlawful
3 activity; or

4 (ii) with intent to engage in conduct constituting a violation of section
5 7201 or 7206 of the Internal Revenue Code of 1986; or

6 (B) knowing that the transaction is designed in whole or in part—

7 (i) to conceal or disguise the nature, the location, the source, the
8 ownership, or the control of the proceeds of specified unlawful activity; or

9 (ii) to avoid a transaction reporting requirement under State or Federal law
10

11 18 U.S.C. § 1956(a)(1).

12 37. Section 1956 also makes it a crime for:

13 Whoever, with the intent—

14 (A) to promote the carrying on of specified unlawful activity;

15 (B) to conceal or disguise the nature, location, source, ownership, or
16 control of property believed to be the proceeds of specified unlawful
17 activity; or

18 (C) to avoid a transaction reporting requirement under State or Federal
19 law,

20 conducts or attempts to conduct a financial transaction involving property
21 represented to be the proceeds of specified unlawful activity, or property
22 used to conduct or facilitate specified unlawful activity

23 18 U.S.C. § 1956(a)(3).

24 38. The statute defines “represented” to mean “any representation made by a
25 law enforcement officer or by another person at the direction of, or with the approval of,
26 a Federal official authorized to investigate or prosecute violations of [money
27 laundering].” *Id.*

39. As set forth below, Wilson has repeatedly demonstrated a willingness to deal in funds that are derived from, or believed to have derived from, criminal activity, including drug trafficking, for the purposes of promoting the criminal activity, concealing the nature and ownership of the proceeds of the unlawful activity, and to avoid transaction reporting requirements.

C. Forfeiture

40. Title 18, United States Code, Section 981 ("civil forfeiture") provides that "[a]ny property, real or personal, involved in a transaction or attempted transaction in violation of section 1956 . . . or 1960 of this title, or any property traceable to such property" is subject to forfeiture to the United States. 18 U.S.C. § 981(a)(1)(A).

41. Title 18, United States Code, Section 982 ("criminal forfeiture") provides that the court, "in imposing sentence on a person convicted of an offense in violation of section 1956 . . . or 1960 of this title, shall order that the person forfeit to the United States any property, real or personal, involved in such offense, or any property traceable to such property." 18 U.S.C. § 982(a)(1).

42. Title 21, United States Code, Section 881 provides that "[t]he following shall be subject to forfeiture to the United States and no property right shall exist in them: . . . All moneys, negotiable instruments, securities, or other things of value furnished or intended to be furnished by any person in exchange for a controlled substance or listed chemical in violation of this subchapter, all proceeds traceable to such an exchange, and all moneys, negotiable instruments, and securities used or intended to be used to facilitate any violation of this subchapter." 21 U.S.C. § 881(a)(6).

43. Title 21, United States Code, Section 853 provides that "[a]ny person convicted of a violation of this subchapter or subchapter II of this chapter punishable by imprisonment for more than one year shall forfeit to the United States . . . any property constituting, or derived from, any proceeds the person obtained, directly or indirectly, as the result of such violation." 21 U.S.C. § 853(a)(1).

//

SUMMARY OF INVESTIGATION

A. The Denver Investigation

44. On or about September 25, 2013, an HSI Denver undercover agent (the "Denver UCA") met with an individual (who was not Wilson) at a residence in Colorado to purchase bitcoins for cash. During the meeting, the individual stated that there was a network of people trading bitcoins on a website called "bitcoin-otc." The individual also stated that the Denver UCA should look up a user that uses the name "Michael]" (later identified as Michail Wilson, a/k/a "Michail1") whom the individual said had a good rating. The Denver UCA asked the individual about anonymity of transactions. In response, the individual referenced "Michael]" and indicated that he/she had trusted "Michael]" with "thousands" of dollars and that the Denver UCA could use the postal system for anonymity. The individual wrote down the username "Michael]" on a piece of paper and provided it to the Denver UCA.

45. The individual later revealed to law enforcement that he/she was a drug vendor on the Silk Road, and that the individual also sold bitcoins for cash. The individual said that Wilson had helped when a customer requested a large amount of bitcoins. According to bank records, that customer wrote Wilson five checks totaling \$117,750 over a few weeks period in April 2013.

46. On or about May 12, 2014, Special Agent ("SA") McWhirter located the website www.michail.com. On that same day, SA McWhirter reviewed the "bitcoin-otc" forum summary page for "Michail1" and noted that the account was registered in July 2, 2011. The page referenced the website "www.michail.com" and listed the user as a male, age 42, in Everett, Washington.

47. In March 2015, the Denver UCA contacted Wilson. Wilson agreed to sell the Denver UCA bitcoins. Under the deal, the Denver UCA agreed to mail Wilson

1 \$11,650 in cash,³ which in fact was delivered by a postal inspector posing as a mail
2 carrier. After Wilson received the cash, he sent the Denver UCA 40.45138888 in
3 bitcoins to an undercover bitcoin wallet address that was provided by the Denver UCA.

4 48. About a week later, on or about March 18, 2015, Wilson contacted the
5 Denver UCA. Wilson mistakenly thought that he had sold the Denver UCA bitcoins the
6 previous day, when in fact it appeared that Wilson was dealing with another customer not
7 associated with law enforcement. Wilson told the Denver UCA: "Would it hurt your
8 feelnigs if I said you were the smallest trade last." Wilson later said he was joking and
9 that the deal was the "2nd biggest" he completed that week.

10 49. In April 2015, Wilson and the Denver UCA discussed another deal. The
11 Denver UCA mentioned that he had been researching a company that exchanges gold for
12 bitcoins. The Denver UCA said he was "see[ing] if it is viable." Wilson said: "It is
13 unless you're trying to avoid tracking." The Denver UCA said that was a concern, to
14 which Wilson replied, "That's why I said to be careful."

15 50. Later that month, Wilson and the Denver UCA discussed another deal, to
16 exchange \$70,000 in cash for bitcoins. Wilson said that he and his "business partner,"
17 "Tim," would join together on the deal. Tim later contacted the UCA, and the two
18 completed the deal in Denver. Tim indicated that Wilson was supplying a portion of the
19 bitcoins that were transferred.

20 51. The Denver UCA and Wilson continued communicating after the deal.
21 Wilson explained that he typically sold bitcoins at spot (*i.e.*, that Wilson sold bitcoins at
22 the then-prevailing marketplace price), and that he had "[n]o problem finding people."
23 He said: "Sometimes, I get people that really want coins even if I don't have them
24 available. So, I get them for a higher price. Example 8-10% over spot. Basically, I keep
25 coins on reserve for such a thing."

26
27
28 ³ As to the transactions conducted between Wilson and undercover agents, described herein, all references to "cash" refer to United States currency.

52. Over the next few months, Wilson made inquiries with the Denver UCA about a potential deal. Wilson periodically sent the Denver UCA pictures of one of his bitcoin wallets, which at one point in October 2015 showed a balance exceeding 722 bitcoins. The value of those coins exceeded \$185,000 at then-prevailing market exchange prices.

B. The Seattle UCA Activity

53. In October 2015, the Denver UCA introduced Wilson to a Seattle-based undercover agent (the "Seattle UCA"). On or about October 23, 2015, the Seattle UCA and Wilson met at a restaurant in the Western District of Washington. Wilson was seen driving the **Target Vehicle**. The Seattle UCA posed as someone interested in purchasing bitcoins for cash. The Seattle UCA said that she was trying to start business up north with Canadians, was worried about moving big piles of cash, and thought that bitcoins might be an option. The Seattle UCA said that bitcoins held appeal because her business could "only hide so much."

54. During the meeting, Wilson explained how bitcoins could be "washed" or "tumbled" to obscure the fact that particular bitcoins were used in criminal activity. Based upon my knowledge and experience, I know that "tumbling," in this context, may involve a process by which individuals can obfuscate transfers of criminally derived bitcoins by mixing such "tainted" bitcoins with legitimate bitcoins. As Wilson explained:

I don't want to go into what you're using them [*i.e.*, the bitcoins that the Seattle UCA was seeking] for but...So a lot of people....Silk Road, drug market, people do that and got to be careful with that, because if I sell you coins, not saying you have anything to do with drugs, but you sell to her, and she does have something to do with drugs, and you put it in her account, and now all of a sudden they backtrack the coins to you, not to you as a person, but to that account, then all of a sudden those coins become tainted. There's nothing they can do to stop it, but now all of a sudden, what if you then take your account and you send more coins to an exchange, you want to be legitimate at that point right? Well if you do that, and they say, "hey that same account was used to buy drugs on the Silk Road market." Now your account, ah, but you went to the exchange, and in order for you to go to an exchange you have to give them your name and

1 address and stuff because, if your exchanging coins for cash to send it to
2 your bank account they know who you are. Then they say to you, "Who is
3 this person over here? Why did you buy drugs?" "I sold them to another
4 fucking Juan" You know what I....So, so then there's tumblers. There's
5 websites that are designed so that way, let's say you have a hundred coins,
6 and you can tumble them. It costs you one and a half percent, right, so, to
7 tumble a coin means you send your coins in, and then me I'm going to send
8 my coins in, this guy, you know thousands of people are sending their coins
9 in. You sent in a hundred so you end up with 98.5 coins back, but it's from
10 everybody. They're not your original coins, and they're from everybody
11 else. So....

12 Seattle UCA: It's kind of a way to wash it.

13 Wilson: Yes. Washing, tumbling, same thing. And then, and then my coins so
14 now, yeah, part of my coins show that it went from your account to her she went
15 to the Silk Road person and whatnot, but it's, it's micro-amounts. So even though
16 you sent in 98 or 100 coins, you're going to get .38 from me and .125 from them
17 and so...now it's impossible to figure out who's what, you know, where did you
18 get if from, why did you tumble them, 'cause you can say, "I don't know, I just
19 sent them into a service because I didn't know...

20 Seattle UCA: ...I thought that's what you do...

21 Wilson: "Yeah, people do that all the time. Ah, the coins that I get are tumbled
22 before I get them. Ah, I don't tumble them myself. Because, I don't.....that's
23 why I was saying the two wallets, the one phone is already tumbled, and it's not
24 tied to any account that's related to my name.

25 55. The Seattle UCA asked Wilson if she should tumble (*i.e.*, wash) any
26 bitcoins that she received from Wilson. Wilson said that there was no need because the
27 bitcoins would already be tumbled. Wilson also said he would never send the Seattle
28 UCA bitcoins from his publicly known address because if she were ever caught doing
something wrong, the bitcoins could not be traced back to Wilson. Rather, the bitcoins
could only be traced to an account that didn't have any of his personal information.

1 Wilson also explained that he regularly established new accounts to limit transaction
2 history. He said he also used the Tor browser⁴ to conceal his presence.

3 56. Wilson went on to explain to the Seattle UCA that he actively avoided
4 registering as a money transmitter. He said:

5 My name is well known, because I have accounts everywhere, I mean
6 separate (unintelligible), because I bought sixty thousand dollars' worth of
7 coin in two purchases, ah, and then saying, and I have a Local bitcoins
8 account, they say I'm buying coins to sell on the market I need to be an
9 MSB, money service businesses, and, uh, once I register as an MSB they'll
10 let me back in. And I told them to go fuck themselves. Ah, I'm not going
11 to register because now with that said I have the burden of proving for taxes
12 and whatnot.

13 57. Wilson also referenced the Denver UCA and said he did not know what the
14 Denver UCA did with the bitcoins and "probably doesn't want to know." Wilson said
15 that he received bitcoins constantly and that a concern of his was dealing with the amount
16 of cash that he exchanges.

17 58. The Seattle UCA asked if Wilson could exchange \$25,000 for bitcoins.
18 Wilson responded, "That's nothing." The Seattle UCA asked Wilson's limit for
19 conducting a transaction, and Wilson said, "\$150,000." Wilson showed the Seattle UCA,
20 via the Mycelium application on the **Samsung Phone**, Wilson's Mycelium Wallet, which
21 showed a balance of bitcoins worth approximately \$180,000.

22 59. On or about October 27, 2015, Wilson and the Seattle UCA met again in
23 the Western District of Washington. The Seattle UCA handed Wilson a bag containing
24 \$25,000 in cash. Wilson then, using the Mycelium application on the **Samsung Phone**,

25 ⁴ "The Onion Router" or "TOR" network is a special network of computers on the Internet, distributed around the
26 world, that is designed to conceal the true Internet Protocol ("IP") addresses of the computers accessing the network,
27 and, thereby, the locations and identities of the network's users. TOR likewise enables websites to operate on the
28 network in a way that conceals the true IP addresses of the computer servers hosting the websites, which are referred
to as "hidden services" on the TOR network. Such "hidden services" operating on TOR have complex web
addresses, which are many times generated by a computer algorithm, ending in ".onion" and can only be accessed
through specific web browser software designed to access the TOR network. Most "hidden services" are considered
dark web services with no legitimate or identified service provider to which legal process may be served.

1 transmitted bitcoins to a wallet that was designated by the Seattle UCA. The Seattle
2 UCA told Wilson that the wallet belonged to the Seattle UCA's boss. In fact, the wallet
3 was an undercover wallet maintained by HSI (and not any individual agent). The Seattle
4 UCA said that her business involved bringing product down in exchange for product
5 going north at a two-to-one exchange. The Seattle UCA said they often were short in
6 product going north and they previously supplemented the difference in cash, but now
7 wanted to try bitcoins because it would be safer. Wilson told the Seattle UCA that he had
8 bitcoins coming into his wallet all of the time, and that it was not a big deal to do a
9 \$25,000 transaction. Wilson said that he did not typically sell at spot, and that he was
10 making very little on the deal with the Seattle UCA.

11 60. On or about November 20, 2015, the Seattle UCA and Wilson met again in
12 the Western District of Washington. The Seattle UCA provided Wilson with \$12,000 in
13 cash in exchange for bitcoins that Wilson transmitted, via the Mycelium application on
14 the **Samsung Phone**, to an undercover HSI wallet (which the Seattle UCA had told
15 Wilson belonged to the Seattle UCA's boss). Wilson said that he always sold at five to
16 ten percent over spot. During the meeting, Wilson explained that he stopped doing
17 business with a particular customer because of New York State's licensing requirements.
18 Wilson explained:

19 It's funny because I used to have a big guy in New York, and uh, he, first
20 time I dealt with him he says, Ok, I've heard about your name, dah dah dah,
21 you know....I don't know if you know who I am or how rated I am...I'm
22 pretty well known for having bitcoins, in over the counter (unintelligible),
23 right, and uh, he says "Hey, can we make a deal for 10 grand?", and I'm
24 like "Sure". So he overnights me 10 grand, and uh I get it to him in bitcoin,
25 he says, "Hey, do you mind if we double it?" I'm like, "No problem." So
26 then boom right again, 20 grand, gets it, send him the coins, "Hey, can we
27 double it?" I'm like, "Sure." So he sends me 40 grand, he says, "Hey do
28 you mind if we make another deal?" I said, "I can't keep doubling." He
says, "Well no, it's gonna be more around 12 grand for now." And...but
then he backed off because uh, he's pretty well known because he has
ATMs in New York.

1 Seattle UCA: Oh really

2 Wilson: So now he has, because it's BitLicensed, right...that came up in New
3 York, now all of a sudden he's become regulated. So the only way he'd be able to
4 buy from me is if it's through the bank, and I'd have to give them my license and
all this other stuff, and I'm like, "Well fuck that!" That's what I said, "Fuck that."

5 61. On or about December 2, 2015, the Seattle UCA and Wilson again met in
6 the Western District of Washington. The Seattle UCA provided Wilson with \$15,000 in
7 cash and Wilson transmitted bitcoins, via the Mycelium application on his **Samsung**
8 **Phone**, to an undercover HSI wallet that Wilson was told belonged to the Seattle UCA's
9 boss. The Seattle UCA said that her boss wanted her to take stuff up north because the
10 Seattle UCA never got hassled at the border. The Seattle UCA said she was reluctant,
11 and only handled the money because she didn't want to get into trouble for the stuff
12 going north.

13 62. On or about May 12, 2016, Wilson and the Seattle UCA met again in the
14 Western District of Washington. The Seattle UCA provided Wilson with \$5,000 in cash
15 and Wilson transmitted bitcoins, via the Mycelium application on his **Samsung Phone**, to
16 an undercover HSI wallet. During the meeting, the Seattle UCA described for Wilson
17 how her organization had a load seized at the border, and that they needed to move a lot
18 of money as a result. The Seattle UCA asked Wilson if he could handle a transaction in
19 the future of about \$50,000 to \$100,000. Wilson said that he could but that he would
20 have to charge closer to the ten percent that he charges other clients. Wilson, referencing
21 the seizure of the "load," commented that one of his former sources of bitcoins was also
22 involved in "that" market. During this meeting and exchange, Wilson mentioned to the
23 Seattle UCA that he normally keeps twenty thousand dollars in his car at all times for
24 buying bitcoins. Wilson arrived to this meeting by motorcycle. He mentioned that he
25 had purchased the bike with bitcoins.

26 63. On or about January 24, 2017, Wilson and the Seattle UCA met again in the
27 Western District of Washington. Wilson was seen driving the **Target Vehicle**. During
28

1 the meeting, Wilson asked the Seattle UCA if her business dealt with “coke,” “molly,” or
2 methamphetamine. The Seattle UCA said that her organization arranges for cocaine to be
3 brought up to Canada from the southern border with the United States, in exchange for
4 bringing Ecstasy down to the United States from Canada. Because the value of the drugs
5 from the south and the north are often not equal, money typically has to be moved to the
6 customer in Canada to make up the difference. The Seattle UCA said that she liked
7 bitcoins because it is much easier to conceal and transfer across the border compared to
8 cash.

9 64. During the meeting, Wilson talked extensively about legitimate bitcoin
10 exchanges (e.g., Coinbase). Wilson said he did not buy bitcoins from these exchanges
11 because they track the bitcoins that they sell and because of “KYC” (referring to “know
12 your customer” rules that financial institutions must follow). Wilson said that he
13 previously bought bitcoins from Coinbase; at the same time, Wilson advertised that he
14 bought and sold bitcoins on LocalBitcoins.⁵ Wilson said that Coinbase found out that
15 Wilson was buying and selling bitcoins and demanded that he register as a money service
16 business, which he refused to do. Wilson told the Seattle UCA that she and her boss
17 should probably ask Wilson about how to make bitcoin transactions anonymous and how
18 to send them to a tumbler. Wilson said that the majority of people he deals with are
19 involved in marijuana and marijuana oil, and are vendors on Alphabay, a website on the
20 dark web that offers for sale drugs, firearms, stolen property, and other contraband.
21 Wilson also mentioned that he dealt in cash to avoid paying taxes. Finally, Wilson
22 admitted that he engaged in “money laundering,” and commented that the less that he
23 knows about his clients the better to maintain plausible deniability.

24
25
26
27 ⁵ LocalBitcoins, OY—and their associated web platform, localbitcoins.com (“LBC”)—is a Finnish company that is
28 not a licensed money transmitting business registered with the U.S. Government and compliant with the Bank
Secrecy Act, which requires establishment and maintenance of anti-money laundering (“AML”) programs in
accordance with KYC rules, such as identifying persons involved in currency transactions over certain thresholds.

1 65. On or about February 10, 2017, the Seattle UCA and Wilson met again in
2 the Western District of Washington to make an exchange. Wilson arrived at the meeting
3 driving the **Target Vehicle**. During the encounter, the Seattle UCA gave Wilson \$20,000
4 in exchange for bitcoins. Wilson offered to provide the Seattle UCA with a contact in
5 Canada who could help exchange for cash the bitcoins that the Seattle UCA was
6 purchasing.

7 66. On or about February 28, 2017, the Seattle UCA and Wilson met again in
8 the Western District of Washington. Wilson was seen driving the **Target Vehicle**. The
9 Seattle UCA provided Wilson with \$20,000 in cash, and, in exchange, Wilson transmitted
10 bitcoins, via the Mycelium application on the **Samsung Phone**, to an undercover wallet
11 that was specified by the Seattle UCA. During the meeting, Wilson said that he that he
12 was "sitting on a ton of cash right now." He said he did not put his money in the bank,
13 but instead stores his cash in a safe that his friend maintains.

14 67. On or about April 17, 2017, the Seattle UCA and Wilson met again in the
15 Western District of Washington. Agents observed Wilson use his left thumbprint to
16 access his **Samsung Phone**, and then access the Mycelium app. Agents later observed
17 Wilson access his **Apple iPhone** by unlocking the phone with his left thumbprint and
18 then accessing the Mycelium app. Wilson talked about the differences between
19 Mycelium on an android smartphone (such as a Samsung phone) compared to Apple, and
20 said he did not like the Apple version. Wilson stated: "I mean I just happen to have coins
21 in it." He showed the Seattle UCA his recent transactions on his Apple Mycelium app,
22 and said they are all "old coins", and the only reason he would use that phone is if he
23 forgot his other (Samsung) phone. Wilson further stated that there is no password to
24 access the Apple Mycelium app, only the password to open the phone. Wilson stated that
25 with his android phone there is a password to get into the phone, as well as a code to open
26 the Mycelium app. Agents were able to observe the passcode that Wilson used to access
27 the Mycelium app on his **Samsung Phone**.

68. During the April 17 meeting, agents observed that Wilson's Mycelium app on his **Samsung Phone** held 156.02748916 worth of bitcoins.⁶ Wilson sold the Seattle UCA 4.03102 in bitcoins for \$5000 in cash. Wilson transmitted the bitcoins to an undercover digital wallet that was specified by the Seattle UCA.

C. The Dark Web Buyer

69. In January 2016, HSI agents conducted a controlled delivery of an international parcel containing approximately 108 grams of suspected Methylenedioxymethamphetamine ("MDMA") to a source of information ("SOI").⁷ The SOI cooperated with law enforcement and stated that he/she ordered the MDMA from a vendor located in Germany via the dark web marketplace website "Neculus." The SOI stated in the past he/she purchased MDMA, Xanax and other drugs from the site. When the SOI was asked about where he/she purchased bitcoins to obtain the drugs, the SOI revealed he/she purchased them in December 2015 from a white male he contacted through the website localbitcoin.com with the moniker "michail1." The SOI revealed he/she met the bitcoin exchanger "michail1" at a McDonald's near Bothell-Everett Highway and Interstate 405. The SOI stated that he/she gave "michail1" cash in exchange for bitcoins. The SOI stated that "michail1" charged him/her 3.5% above the market value of bitcoin for the deal. The SOI also recalled that "michail1" drove a small, dark-colored sports utility vehicle. A review of the SOI's cellular phone revealed communications with "michail1" using the email address michail1@aol.com. This email address had been previously identified via search warrant by HSI Denver as belonging to Michail Wilson.

//

⁶ As of June 6, 2017, the website www.coindesk.com/calculator/ estimates that 156 bitcoins is the equivalent of \$448,329.96 in U.S. currency.

⁷ The Court should assume that the SOI could be impeached for a variety of reasons, including criminal history, substance abuse, and incentives to cooperate.

D. Mail Intercept

70. On March 25, 2014, postal inspectors conducted an Express Mail interdiction located at the United States Postal Service (USPS), Seattle Processing and Delivery Center. The inspectors utilized the assistance of Drug Enforcement Administration Task Force Officer Bruchs and drug-K9 Lilly. During the interdiction, Express Mail parcel EK244310942US addressed to Technology Express, Attention Michail WILSON, 22122 20th Ave SE, Suite 164, Bothell WA 98021, with a return address of "Jeff Wheeler, 920 Bayside Lane #4, Tampa, FL 33637," was identified as having a return address with a fictitious name and address after searching USPS and law enforcement databases. The parcel placed in a line up with other controlled parcels for K9 Lilly to perform a free air sniff. K9 Lilly indicated a positive alert on the parcel.

71. On March 25, 2014, Postal Inspector Willyerd conducted a knock and talk at the Technology Express business. The inspector spoke with Wilson who indicated he was the owner of Technology Express and provided verbal consent to open the parcel. After opening the parcel, the inspector discovered \$1730 in cash in the parcel.

72. WILSON stated that the cash inside the parcel was payment for a larger purchase for bitcoin mining equipment (5 chip/ dual mode/ SHA 526). Wilson further stated he did not know "Jeff Wheeler" or if he lived in Tampa, Florida. Wilson said he only knew the sender of the parcel from a bitcoin chat forum. During the conversation with Wilson about the cash and the bitcoin chat forum he indicated towards the computer inside his work area of the business, Technology Express, as to where he was communicating on the bitcoin chat forum.

E. Wilson's Purchases of Bitcoins at Below-Market Value

73. As outlined above, Wilson has made various statements to undercover law enforcement agents about the prices at which Wilson purchases or sells bitcoins. In

1 February 2015, Wilson exchanged text messages with a cooperating defendant.⁸ During
 2 the text exchanges, Wilson said that he acquires bitcoins at below-market value.
 3 Specifically, he said, "Well, I get [bitcoins] at 8% under from the time it is sent. No
 4 questions." Wilson further said: "It's determined by going to the transaction on
 5 blockchain.info click on the price and you and see the price at time of transaction. cut
 6 back 8% is what I pay." Later, in a meeting on or about January 23, 2017, with the
 7 Seattle UCA, Wilson said, "I buy it [i.e., bitcoins] at about 8 percent below value, and
 8 sell for about 8 percent above value; I make 16 points."

9 74. Based on my training and experience, I submit that it highly likely that
 10 Wilson is able to acquire bitcoins at such a steep discount because the bitcoins he
 11 acquires were involved in illegal transactions and therefore carry the risk that their
 12 ownership will bring law enforcement attention. By way of contrast, Coinbase, a
 13 legitimate bitcoin exchange, typically sells bitcoins at their market price (plus a small
 14 service fee of approximately 1.49%).

15 SEARCHES AND SEIZURES

16 **A. The Subject Business**

17 75. The **Subject Business** is believed to be a functioning company that
 18 conducts legitimate business and is owned by a non-target of this investigation. As set
 19 forth below, Michail Wilson, the target of this investigation, is believed to be an
 20 employee of the **Subject Business**.

21 76. As of April 5, 2017, Washington Department of Revenue records indicated
 22 that the **Subject Business** was located at a particular location in Bothell, Washington.
 23 During the course of the investigation, Wilson was seen repeatedly either departing from,
 24 or returning to, that location after meeting with the Seattle UCA (namely on or about
 25
 26
 27

28 ⁸ The Court should assume that the cooperating defendant could be impeached for a variety of reasons, including criminal history, substance abuse, and incentives to cooperate.

1 October 27, 2015, November 20, 2015, December 2, 2015, May 12, 2016, and January
2 24, 2017).

3 77. In addition, as described above, Wilson admitted using his computer to
4 communicate about bitcoins at the previous address for the **Subject Business**.

5 78. It is my belief, based on the foregoing, and my training and experience, that
6 Wilson likely conducts part of his bitcoin business while at work. I believe it is likely
7 that he would generate hard-copy and paper documents related to his business, such as
8 receipts, records of cash transactions, and other items specified in Attachment B, and that
9 there is probable cause to believe that the **Subject Business** would be the place those
10 items would be stored.

11 79. During the course of the investigation, the **Subject Business** moved from
12 the Bothell location to its current location in Woodinville, Washington (further described
13 in Attachment A-1). Specifically, in or about February 2017, agents observed that the
14 sign depicting "Technology Express" had been removed from the Bothell, Washington
15 location. On or about February 28, 2017, the **Target Vehicle** was observed at the newer
16 Woodinville premises of the **Subject Business**. Wilson was later observed departing, via
17 the **Target Vehicle**, the Woodinville premises of the **Subject Business** and driving to a
18 parking lot elsewhere in Woodinville to meet the Seattle UCA. As described above,
19 during this meeting the Seattle UCA gave Wilson \$20,000 in exchange for bitcoins that
20 Wilson transmitted to a wallet designated by the Seattle UCA. After the meeting
21 concluded, Wilson drove back to the Woodinville premises of the **Subject Business**.

22 80. On or about March 24, 2017, I obtained a tracking warrant for the **Target**
23 **Vehicle**, and it was installed two days later. During the period that the tracking device
24 was active, Wilson regularly traveled to and from the **Subject Business** each weekday.

25 81. Agents plan to execute the warrant by asking the **Subject Business** for the
26 area(s) of the business' premises that are directly linked to Wilson, such as his cubicle,
27 and to limit the search to those areas. Agents do not plan to search any digital devices
28 pursuant to this warrant at this location, however, agents do intend to seize any devices

1 that are specifically designed to serve as bitcoin wallets—such as devices sold by Trezor
2 or Ledger—and seek, as appropriate, follow-up warrants from the Court. As with any
3 search warrant, I expect that this warrant will be executed reasonably. Agents also will
4 take steps to ensure that normal business operations are not unduly interrupted.

5 **B. The Target Vehicle**

6 82. During this investigation, law enforcement agents have repeatedly
7 observed Wilson using the **Target Vehicle**. In particular, he was seen driving the **Target**
8 **Vehicle** to and/or from several of the meetings with the Seattle UCA that are described
9 above, including those on or about April 30, 2015, October 23, 2015, January 23, 2017,
10 February 10, 2017, and February 28, 2017.⁹ As previously mentioned, the **Target**
11 **Vehicle** is registered to Wilson.

12 83. On February 28, 2017, Wilson said to the Seattle UCA that she should buy
13 some bitcoins for herself. Wilson said, “You can’t go and buy a new car with it.... I
14 mean that’s how I bought that but...” Wilson was pointing to the **Target Vehicle** when
15 he made that comment.

16 84. On the basis of the evidence described herein, I submit that there is
17 probable cause to believe that the **Subject Vehicle** constitutes property involved in a
18 violation of 18 U.S.C. § 1956 and 18 U.S.C. § 1960, or is traceable to such property. I
19 further submit that there is probable cause to believe that the **Subject Vehicle** constitutes
20 property constituting, or derived from, proceeds obtained, directly or indirectly, as the
21 result of drug trafficking.

22 85. Here, because the **Target Vehicle** is mobile and can be easily moved,
23 concealed, or transferred, a protective order under 21 U.S.C. § 853(e) may not be
24 sufficient to ensure that the **Target Vehicle** remains available for forfeiture.

25 //

26
27
28 ⁹ On October 27, 2015, and November 20, 2015, Wilson arrived in a rental car, explaining that the **Target Vehicle** was being repaired.

1 **C. The Samsung Phone and the Apple iPhone**

2 86. As set forth above, during the course of the investigation, agents have
3 repeatedly observed Wilson using the **Samsung Phone**, and also observed him use the
4 **Apple iPhone**, in connection with his bitcoin business.

5 87. In addition, as set forth above, during the investigation, Wilson has
6 exchanged texts with undercover agents regarding his scheme since 2013. It is not clear
7 what phone Wilson used to exchange texts, but the formatting of the messages indicates
8 that they were sent from an Apple-brand iPhone. Wilson did engage in communications
9 with the Denver UCA using Signal, an encrypted messaging application. Wilson also
10 primarily communicated with the Seattle UCA using Signal.

11 88. I also know, based on my training and experience, that persons engaged in
12 the type of business that Wilson is engaged in, often will exchange texts in connection
13 with bitcoin deals. For example, persons will often exchange texts regarding meeting
14 times and locations, as well as deal prices.

15 **D. The Mycelium Bitcoins**

16 89. On the basis of the evidence described herein, I submit that there is
17 probable cause to believe that the **Mycelium Bitcoins** constitute property involved in a
18 violation of 18 U.S.C. § 1956 and 18 U.S.C. § 1960, or are traceable to such property. I
19 further submit that there is probable cause to believe that the **Mycelium Bitcoins**
20 constitute property constituting, or derived from, any proceeds obtained, directly or
21 indirectly, as the result of drug trafficking.

22 90. I know that individuals associated with the business of transferring bitcoins
23 often have safeguards in place to ensure that their bitcoins become further secured in the
24 event that their bitcoins become potentially vulnerable to seizure and/or unauthorized
25
26
27
28

1 transfer. As such, a protective order under 21 U.S.C. § 853(e) may not be sufficient to
 2 ensure that the **Mycelium Bitcoins** remains available for forfeiture.¹⁰

3 **E. Accessing the Samsung Phone and the Apple iPhone**

4 91. I know from my training and experience, as well as from information found
 5 in publicly available materials including those published by Samsung and Apple, that
 6 some models of Samsung and Apple devices offer their users the ability to unlock the
 7 devices via the use of a fingerprint or thumbprint (collectively, "fingerprint") in lieu of a
 8 numeric or alphanumeric passcode or password. This feature is sometimes called, and
 9 for the purposes of this affidavit is referred to as, "Touch ID."¹¹

10 92. If a user enables Touch ID on a given Apple or Samsung device, the user
 11 can register fingerprints that can be used to unlock that device. The user can then use any
 12 of the registered fingerprints to unlock the device by pressing the relevant finger(s) to the
 13 device's Touch ID sensor. As set forth above, Wilson was observed using his thumbprint
 14 to unlock both the **Samsung Phone** and the **Apple iPhone**.

15 93. In my training and experience, users of Apple and Samsung devices that
 16 offer Touch ID often enable it because it is considered to be a more convenient way to
 17 unlock the device than by entering a numeric or alphanumeric passcode or password, as
 18 well as a more secure way to protect the device's contents. This is particularly true when
 19 the user(s) of the device are engaged in criminal activities and thus have a heightened
 20 concern about securing the contents of the device.

21 94. In some circumstances, a fingerprint cannot be used to unlock a device that
 22 has Touch ID enabled, and a passcode or password must be used instead. For Apple
 23 devices, these specific circumstances include: (1) when more than 48 hours has passed
 24 since the last time the device was unlocked and (2) when the device has not been
 25 unlocked via Touch ID in 8 hours and the passcode or password has not been entered in
 26

27 ¹⁰ I seek authorization to search the phones that are the subject of this affidavit for the presence of any other bitcoin
 28 wallets, and to follow-up with additional seizure warrants to the extent necessary and appropriate.

¹¹ As a technical matter, Samsung uses a different term for its fingerprint scanner.

1 the last 6 days. I understand that Touch ID will not unlock a Samsung phone under
2 similar circumstances.

3 95. Thus, in the event law enforcement encounters a locked Samsung or Apple
4 device, the opportunity to unlock the device via Touch ID exists only for a short time.
5 Touch ID also will not work to unlock the device if (1) the device has been turned off or
6 restarted; (2) the device has received a remote lock command; and (3) five unsuccessful
7 attempts to unlock the device via Touch ID are made.

8 96. The passcode(s) or password(s) that would unlock the **Samsung Phone**
9 and/or **Apple iPhone** devices found during the searches described herein are not known
10 to law enforcement. Thus, it will likely be necessary to press the fingers of the user of
11 the **Samsung Phone** and **Apple iPhone** to the respective device's Touch ID sensor in an
12 attempt to unlock the device for the purpose of executing the searches and seizures
13 authorized by the requested warrants. Attempting to unlock the relevant devices via
14 Touch ID with the use of the fingerprints of the user is necessary because the government
15 may not otherwise be able to access the data and bitcoins contained on those devices for
16 the purpose of executing the search and seizures that are the subject of this affidavit.

17 97. I further know that time will be of the essence in securing any bitcoins that
18 are to be seized from Wilson. I know that individuals associated with the business of
19 bitcoin transferring often will have safeguards in place to ensure that their bitcoins
20 becomes further secured in the event that their bitcoins become potentially vulnerable to
21 seizure and/or unauthorized transfer.

22 98. Due to the foregoing, I request that the Court authorize law enforcement to
23 press the fingers (including thumbs) of Michail Wilson to the Touch ID sensors of the
24 **Samsung Phone** and **Apple iPhone** for the purpose of attempting to unlock the devices
25 via Touch ID in order to execute the searches and/or seizures authorized by the requested
26 warrants.

27 //

28 //

Affidavit of Special Agent Patterson - 29
USAO 201501195

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

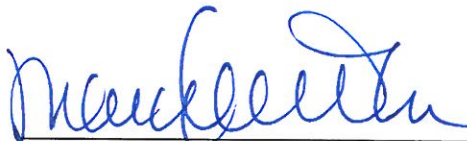
SEALING REQUEST

99. It is respectfully requested that the Court issue an order sealing, until further order of the Court, all papers submitted in support of the requested warrants, including the application, this affidavit, the attachments, and the requested warrants. I believe that sealing these documents is necessary because the information to be seized is relevant to an ongoing investigation and includes references to cooperating individuals. Premature disclosure of the contents of the application, this affidavit, the attachments, and the requested warrants may adversely affect the integrity of the investigation, including giving targets a chance to destroy evidence or take other steps to hinder the investigation.



ROBERT C. PATTERSON
Special Agent
Homeland Security Investigations

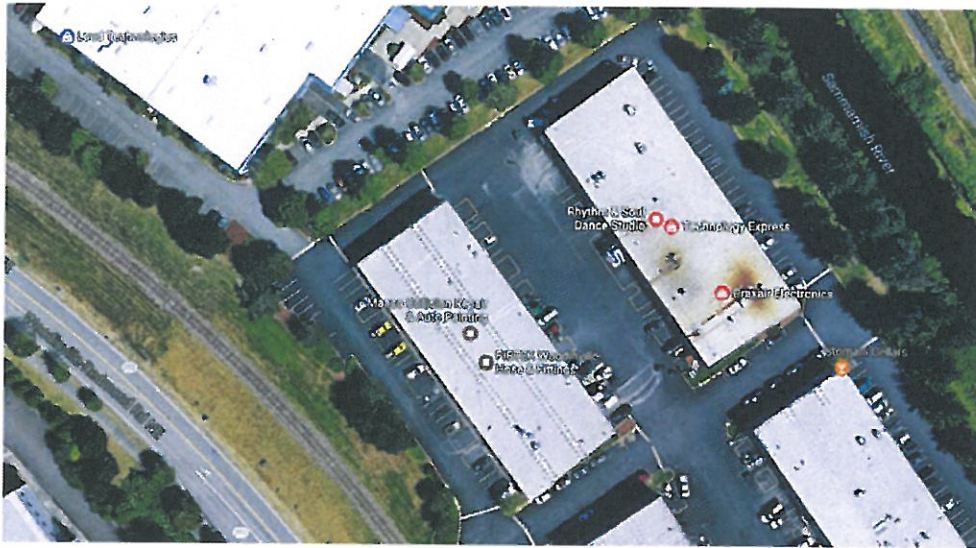
SUBSCRIBED AND SWORN before me this 12 day of June, 2017



MARY ALICE THEILER
United States Magistrate Judge

ATTACHMENT A-1
Place To Be Searched

The place to be searched is the business known as “Technology Express,” located at 16130 Woodinville-Redmond Road, Unit 1, Woodinville, Washington, 98072 (the “**Subject Business**”). The **Subject Business** is further described as located in the northern-most two-story building, and Unit 1 is located in the northern most corner of the building. There is a glass front door to the business with the sign “Unit 1” above the door, and a paper sign taped to the door that says “Technology Express” along with the address and telephone number. The building is regular concrete with grey metal siding. At the rear of the building is a metal door as well as a rollup-style garage door. Taped to the metal door is a sign that states “Technology Express,” along with the address. A picture of the place to be searched is below:



ATTACHMENT A-2

Place To Be Searched

The place to be searched is a maroon 2013 Land Rover Evoque, personalized Washington license plate MICHAIL, registered to Michail Wilson, 12721 50th Ave SE, Everett, Washington 98208, Vehicle Identification Number SALVT1BG8DH810540 (the **"Target Vehicle"**).

ATTACHMENT A-3

Place To Be Searched

The place to be searched is a Samsung telephone that belongs to Michial Wilson.
This warrant authorizes the search of Michial Wilson's person for the cellular phone.

ATTACHMENT A-4

Place To Be Searched

The place to be searched is an iPhone telephone that belongs to Michial Wilson.
This warrant authorizes the search of Michial Wilson's person for the cellular phone.

Attachment B-1

List of Items to be Searched for and Seized

This warrant authorizes the government to search for the following items:

Evidence and/or fruits of the commission of the following crimes: 18 U.S.C. § 1956 (money laundering) and 18 U.S.C. § 1960 (conducting an unlicensed money transmitting business), *i.e.*, the following records, in hard copy or paper form:

- a. any and all documents, records, or information relating to the transfer, distribution, acquisition, purchase, sale, possession, tracking or disposition of virtual currency;
- b. any and all documents, records or information relating to the operation of money transmitting businesses;
- c. any and all documents, records, or information relating to the access, creation and maintenance of websites and hidden (Tor-based) services;
- d. any and all documents, records, or information relating to email accounts used in furtherance of these offenses;
- e. any and all records of any address and/or telephone books, rolodex indicia, electronic organizers, telephone paging devices and the memory thereof, and any papers, records or electronic data reflecting names, addresses, telephone numbers, pager numbers of co-conspirators, sources of virtual currency, identifying information for customers purchasing or selling virtual currency;
- f. any and all applications, documents, records, or information relating to communication with the Financial Crimes Enforcement Network ("FinCEN") or the Washington Department of Financial Institutions ("DFI");
- g. all bank records, checks, credit card bills, account information, safe deposit box information, and other financial records;
- h. all copies of income tax returns filed with the Internal Revenue Service ("IRS") or the Washington DFI.

Attachment B-2

List of Items to be Searched for and Seized

This warrant authorizes the government to search for the following items:

Evidence and/or fruits of the commission of the following crimes: 18 U.S.C. § 1956 (money laundering) and 18 U.S.C. § 1960 (conducting an unlicensed money transmitting business), *i.e.*, the following records, in hard copy or paper form:

- a. any and all documents, records, or information relating to the transfer, distribution, acquisition, purchase, sale, possession, tracking or disposition of virtual currency;
- b. any and all documents, records or information relating to the operation of money transmitting businesses;
- c. any and all documents, records, or information relating to the access, creation and maintenance of websites and hidden (Tor-based) services;
- d. any and all documents, records, or information relating to email accounts used in furtherance of these offenses;
- e. any and all records of any address and/or telephone books, rolodex indicia, electronic organizers, telephone paging devices and the memory thereof, and any papers, records or electronic data reflecting names, addresses, telephone numbers, pager numbers of co-conspirators, sources of virtual currency, identifying information for customers purchasing or selling virtual currency;
- f. any and all applications, documents, records, or information relating to communication with the Financial Crimes Enforcement Network ("FinCEN") or the Washington Department of Financial Institutions ("DFI");
- g. all bank records, checks, credit card bills, account information, safe deposit box information, and other financial records;
- h. all copies of income tax returns filed with the Internal Revenue Service ("IRS") or the Washington DFI.

Attachment B-3

List of Items to be Searched for and Seized

This warrant authorizes the government to search for the following items:

Evidence and/or fruits of the commission of the following crimes: 18 U.S.C. § 1956 (money laundering) and 18 U.S.C. § 1960 (conducting an unlicensed money transmitting business), *i.e.*,

- a. Assigned number and identifying telephone serial number (ESN, MIN, IMSI, or IMEI);
- b. Stored list of recent received, sent, and missed calls;
- c. Stored contact information;
- d. Stored text messages.

During the execution of the warrant, law enforcement personnel are authorized to press the fingers (including thumbs) of Michail Wilson to the fingerprint sensor of the phone to be searched for the purpose of attempting to unlock the device in order to search and seize items as authorized by this warrant. Law enforcement can also search the phone for the presence any bitcoin wallets.

Attachment B-4

List of Items to be Searched for and Seized

This warrant authorizes the government to search for the following items:

Evidence and/or fruits of the commission of the following crimes: 18 U.S.C. § 1956 (money laundering) and 18 U.S.C. § 1960 (conducting an unlicensed money transmitting business), *i.e.*,

- a. Assigned number and identifying telephone serial number (ESN, MIN, IMSI, or IMEI);
- b. Stored list of recent received, sent, and missed calls;
- c. Stored contact information;
- d. Stored text messages.

During the execution of the warrant, law enforcement personnel are authorized to press the fingers (including thumbs) of Michail Wilson to the fingerprint sensor of the phone to be searched for the purpose of attempting to unlock the device in order to search and seize items as authorized by this warrant. Law enforcement can also search the phone for the presence any bitcoin wallets.